A Biblometric review of the Current State and Future Perspectives of XSS attack detection in Web based Applications

Akshat Gaurav, Domenico Santaniello, Avadhesh Kumar Gupta, and Francesco COLACE

***Abstract*—The purpose of this study is to provide a bibliometric overview of the detection of XSS attacks using latest cutting-edge technologies such as artificial intelligence, machine learning, big data, etc. Scopus databases were searched for articles published in English between 2009 and 2022 to discover current trends and concerns about XSS attack detection. A total of 184 empirical and non-empirical studies were compiled as a result of the evaluation process. This study used qualitative computer-assisted data analysis techniques. During the study period, the number of articles published in scientific journals increased exponentially, indicating that the research topic is still in the development phase. The most productive and relevant journals, nations, and authors are listed using bibliometric performance metrics. It also highlights the most important research trends, allowing numerous new research lines to be proposed via visual mapping of Thematic Maps. This study makes an important contribution to the field of sustainable entrepreneurship, providing a comprehensive overview of the field's evolution and current status, as well as a comprehensive, synthesized, and organized summary of the various perspectives, definitions, and trends in the field.**

***Index Terms*—XSS attack, artificial intelligence, machine learning, big data, blockchain.**

I. Introduction

More and more programs and services can be found online for the convenience of the end user [1], [2]. However, these new services and applications have a number of security flaws that can be exploited [3], [4], [5], [6]. Organizations might face serious consequences if cyber thieves exploit these vulnerabilities, which are attractive to digital crooks [7], [8]. The majority of attacks on the Internet are caused by security flaws in its application architecture [9], such as incorrect input validations, insufficient security controls, etc. Cross-Site Scripting (XSS) [10], [11], [12], [13], [6], [14], [15] is the most widely exploited vulnerability on the Internet other then DDoS attack [16], [17], [18], [19], [20], [21], [22], [23], [24], [25] and phishing attack [26], [27]. It's possible for an attacker to introduce malicious code into a legitimate web application using an XSS vulnerability. An attacker might exploit an input vulnerability in a web application to spread malicious code by exploiting XSS [28], [29], [30], [31], [32], [33], [34], [35]. More serious assaults like as phishing, keylogging, cookie stealing, and the like may be carried out on the network as a result of these intrusions. XSS attacks may be used in a variety of ways to get access to the private information of legitimate users. There are three primary types of cyberattacks [36], [37]. That is, reflected XSS, stored XSS, and DOM-based XSS are examples. In comparison to reflected XSS, the stored XSS flaws are more difficult to identify [38].Thus, researchers are working for the detection and identification of different types of cyber attacks [39], [40], [41], [42], [43], [44], [45], [45].

Currently, OSN (online social network)[46], [47], [48], [49], [50], [51], [52] is one of the most widely used internet services. Allows for communication and knowledge exchange between people. Yet in terms of safety, OSN has emerged as the preferred victim of cybercriminals and faces several risks, such as cross-site scripting (XSS) assaults [53], [54], [55]. In this context, authors in [56] offer a new method for detecting XSS in OSN [57], [58], [59], [60] that relies on machine learning [61], [62], [63], [64], [65]. Detecting XSS begins with a novel way for capturing characteristics from online pages and building classification models. To develop our site database, authors use a new way to mimic the propagation of XSS worms. To evaluate our categorization models, we conducted tests on our test database. It is clear from the results of the experiment that our method is an effective way to identify XSS attacks. Web applications are the most often targeted by cybercriminals, with the most common attack vector being Cross-Site Scripting (XSS). The primary strategy for preventing XSS harm at the source code level is a code audit. Manual audits and rule-based audit technologies, on the other hand, have a number of limitations. Machine learning [66] is a new study area in the era of big data that may help with manual auditing [67]. One of the most often occuring vulnerabilities is XSS, or cross-site scripting. XSS may have a wide range of effects, from minor to disastrous. However, XSS detection remains an outstanding problem. Previously, cross-site scripting was addressed with using both static and dynamic analysis. Because of the wide variety of XSS payloads, neither method is impenetrable. As a result of this research,the authors [68] have suggested the use of Genetic Algorithm (GA) [50], [69], [70] and Reinforcement Learning (RL) to combat XSS assaults. Real-world XSS assaults are used to test the suggested method's performance. Our technique outperforms others previously published in the literature, according to the results. As a bonus, our solution is more adaptable to changes in XSS payloads, as well as more intelligible to end users. When the number of attacks increases, our strategy also

Akshat Gaurav, Ronin Institute, Montclair, USA, Email: akshat.gaurav@ieee.org

Domenico Santaniello, University of Salerno, Italy Email: dsantaniello@unisa.it

Avadhesh Kumar Gupta Unitedworld School of Computational Intelligence, Karnavati University (Gujarat)- INDIA Email: dr.avadheshgupta@gmail.com

Francesco COLACE, University of Salerno, Italy Email: fcolace@unisa.it

improves. Detecting Web application assaults using machine learning approaches is becoming more prevalent and providing better results. Injection attacks such as cross-site scripting are common in online applications. Unknown XSS assaults can only be detected using machine learning [71], [72], [73], [74], [75], [76], [77], [78] approaches, which are more effective than current solutions like filter-based, dynamic analysis and static analysis. Machine learning algorithms used to identify XSS assaults include problems such as single base classifiers, limited datasets, and imbalanced datasets in existing research. A large labelled and balanced dataset was used to train supervised ensemble learning algorithms to identify XSS assaults [79].

According to the following structure, the rest of the paper is laid out. Methodology and results are presented in Sections II and III. The paper comes to a close in Section IV.

II. Methodology

A detailed literature study was conducted to determine the effect of cutting-edge technologies on XSS attack detection. The PRISMA review method was used to guide the review process. Systematic reviews are a different research strategy for the systematic and reproducible analysis and synthesis of current research materials. The following are the steps used to write this paper: The selection of the database, the modification of the research criteria, the coding of recovered material, and the evaluation of the information were all part of this process.

A. Eligibility Criteria

Research on the impact of cutting-edge technology on the detection of XSS attacks was included in the review. Publications published between November 2009 and 2022 in English were included in the map to show the current state of research around the world.

B. Restrictions

A limited number of publications were rejected from consideration because they did not fit the research focus. As an example, we do research only in computer science and not in any other discipline.

C. Data Source

Using the Scopus bibliographic database, the data was gathered in May 2022. The following two keywords were included in the search strategy to answer the research question.

- XSS of cross-site scripting
- AI or artificial intelligence
- Machine learning
- Blockchain
- Big data

D. Search Query Selection

In order to obtain information from the Scopus database, we used the following query :

TITLE-ABS-KEY ((xss OR ”Cross Site Scripting” OR ”Cross-Site Scripting”) AND (ai OR ”artificial intelligence” OR ”machine learning” OR ”deep learning” OR ”big data” OR ”blockchian”))

E. Tools Used

VOSviewer (v1.6) and R language were used to analyze the data. The tools provides visual representations of networks that connect nations, institutions, journals, authors, and keywords, making it easier to analyze and understand these connections. Science mapping research can be carried out using the R language, which is based on the science mapping analytic technique that allows longitudinal investigations. Another benefit of using this method is that it helps researchers discover connections and interactions between previously studied topics and new areas of study.

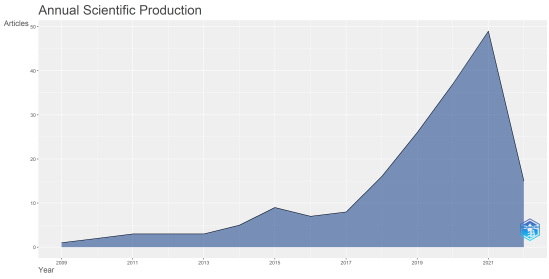
III. Results and Discussion

Studies of an area’s bibliography may provide light on how the topic has developed and point to potential directions for future study. It provides a bird’s eye perspective of several facets of an area. This section is separated into two subsections for the sake of a more thorough study. An overview of scientific output over time is provided, as well as a breakdown by topic area and publication venue of the most widely cited publications, institutes, and authors. Furthermore, we examine the content findings to identify the most important trends in the growth of the retail sector.

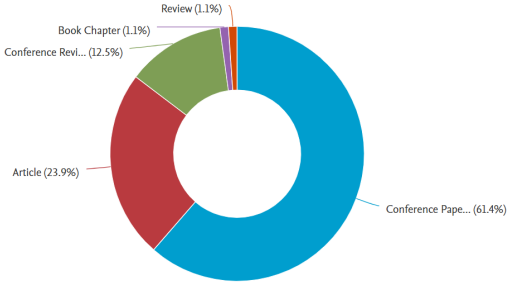
The impact of cutting-edge technologies on XSS attack detection is a significant field of study. Details of our database are represented in Table I. As represented in Table I, our dataset includes 184 articles from 2009 to 2022, these 184 articles have 5.902 citations per document. Furthermore, there are more than 477 unique authors who published papers during this time; therefore, we can say that XSS attack detection through cutting edge technologies is an interesting topic because many authors are working on it. From Figure 1, most of the computer science researchers work in the respective research field.

TABLE I: Overview of Dataset

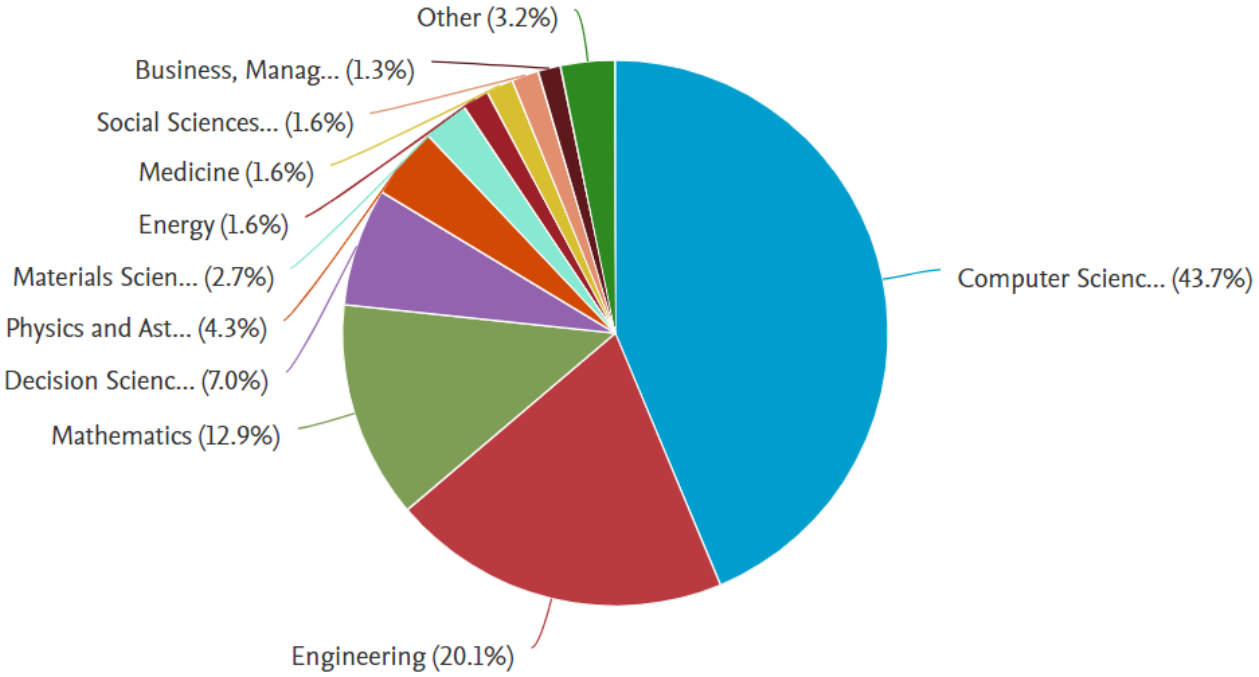
Parameter	Details
Time- Period	2009:2022
Sources	123
Papers	184
References	4329
article	44
book chapter	2
conference paper	113
conference review	23
review	2
Keywords Plus (ID)	997
Authors	477
Single-authored documents	29
Collaboration Index	3.03



(a) Scientific Production



(b) Type of source distribution



(c) Subject distribution

Fig. 1: Database specifications

A. *Distribution of Source*

In this subsection, we give an analysis of the publication sources. To represent the productivity and impact of sources, we use the number of citations, the number of documents published, the h index, the g index, and the m index as comparative variables. Therefore, the top 10 productive sources are represented in Table III. From Table III it is clear that the most productive source is *PROCEEDINGS - INTERNATIONAL SYMPOSIUM ON SOFTWARE RELIABILITY ENGINEERING, ISSRE* with the highest number of citations. The other most popular and quantity-based journals are as follows: *PROCEEDINGS - INTERNATIONAL SYMPOSIUM ON SOFTWARE RELIABILITY ENGINEERING, ISSRE, IEEE ACCESS, ACM INTERNATIONAL CONFERENCE PROCEEDING SERIES, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, LECTURE NOTES IN COMPUTER SCIENCE (INCLUDING SUBSERIES LECTURE NOTES IN ARTIFICIAL INTELLIGENCE AND LECTURE NOTES IN BIOINFORMATICS), ADVANCES IN INTELLIGENT SYSTEMS AND COMPUTING, INFORMATION AND SOFTWARE TECHNOLOGY, PROCEEDINGS - 2011 INTERNATIONAL CONFERENCE ON NETWORK-BASED INFORMATION SYSTEMS, NBIS 2011 JOURNAL OF INFORMATION PROCESSING SYSTEMS, PROCEEDINGS - IEEE SYMPOSIUM ON COMPUTERS AND COMMUNICATIONS.*

1) Source Ranking according to Bradford law: One of the most significant bibliometric laws is Bradford's law. When there is an increase in the number of "subject" papers, there must be an increase in the number of "journals/information sources," according to Bradford's rule. As the Bradford multiplier increases, so does the number of groups of journals that must be involved in order for almost equal numbers of papers to be published in each. Consequently, if the area of study is

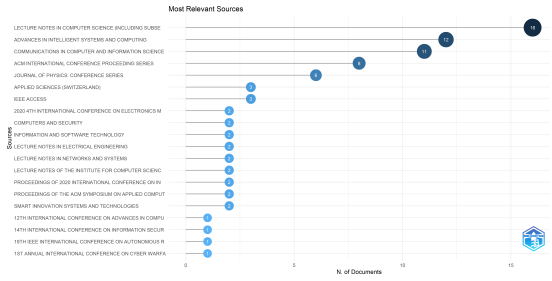
TABLE II: Local Source Impact Details

Element	H Index	G Index	M Index	TC	NP	Paper Year
PROCEEDINGS - INTERNATIONAL SYMPOSIUM ON SOFTWARE RELIABILITY ENGINEERING, ISSRE	1	1	0.076923077	82	1	2010
IEEE ACCESS	3	3	0.75	75	3	2019
ACM INTERNATIONAL CONFERENCE PROCEEDING SERIES	4	6	0.444444444	73	6	2014
IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING	1	1	0.125	66	1	2015
LECTURE NOTES IN COMPUTER SCIENCE (INCLUDING SUBSERIES LECTURE NOTES IN ARTIFICIAL INTELLIGENCE AND LECTURE NOTES IN BIOINFORMATICS)	6	7	0.545454545	63	9	2012
ADVANCES IN INTELLIGENT SYSTEMS AND COMPUTING	5	6	0.5	52	6	2013
INFORMATION AND SOFTWARE TECHNOLOGY	1	1	0.1	49	1	2013
PROCEEDINGS - 2011 INTERNATIONAL CONFERENCE ON NETWORK-BASED INFORMATION SYSTEMS, NBIS 2011	1	1	0.083333333	48	1	2011
JOURNAL OF INFORMATION PROCESSING SYSTEMS	1	1	0.166666667	46	1	2017
PROCEEDINGS - IEEE SYMPOSIUM ON COMPUTERS AND COMMUNICATIONS	1	1	0.090909091	42	1	2012
AD HOC NETWORKS	1	1	0.25	40	1	2019
PROCEEDINGS OF 2011 3RD INTERNATIONAL CONFERENCE ON AWARENESS SCIENCE AND TECHNOLOGY, ICAST 2011	1	1	0.083333333	37	1	2011
COMPUTER NETWORKS	1	1	0.333333333	34	1	2020
PROCEEDINGS - 2015 INTERNATIONAL CONFERENCE ON CYBER-ENABLED DISTRIBUTED COMPUTING AND KNOWLEDGE DISCOVERY, CYBERC 2015	1	1	0.125	31	1	2015
PROCEEDINGS - 16TH IEEE INTERNATIONAL CONFERENCE ON HIGH PERFORMANCE COMPUTING AND COMMUNICATIONS, HPCC 2014, 11TH IEEE INTERNATIONAL CONFERENCE ON EMBEDDED SOFTWARE AND SYSTEMS, ICESS 2014 AND 6TH INTERNATIONAL SYMPOSIUM ON CYBERSPACE SAFETY AND SECURITY, CSS 2014	1	1	0.111111111	23	1	2014
PROCEEDINGS OF THE 2015 12TH INTERNATIONAL JOINT CONFERENCE ON COMPUTER SCIENCE AND SOFTWARE ENGINEERING, JCSSE 2015	1	1	0.125	23	1	2015
PROCEEDINGS - 2016 IEEE SYMPOSIUM ON SECURITY AND PRIVACY, SP 2016	1	1	0.142857143	20	1	2016
PROCEEDINGS - 2017 IEEE/ACM 39TH INTERNATIONAL CONFERENCE ON SOFTWARE ENGINEERING, ICSE 2017	1	1	0.166666667	18	1	2017
APPLIED SCIENCES (SWITZERLAND)	2	3	0.666666667	17	3	2020
JOURNAL OF INTERNET SERVICES AND APPLICATIONS	1	1	0.25	17	1	2019

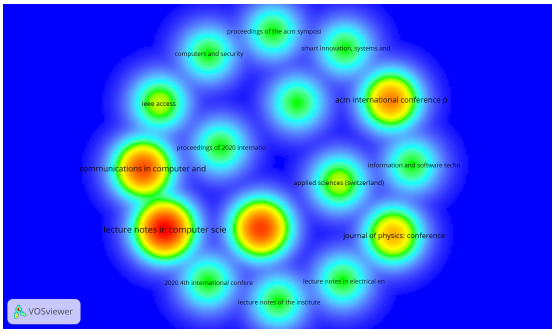
confined, only a small number of journals will be required to provide the core of the work. The number of journals necessary to generate the number of publications grows rapidly beyond the nucleus or first zone. For example, if the next 300 articles are to be supplied by two journals, a total of sixteen journals are required to do so. As represented in Figure 2d the most important and valuable sources are represented in zone 1 of the Bradford figure. Hence, from the above discussion, we can say that *LECTURE NOTES IN COMPUTER SCIENCE (INCLUDING SUBSERIES LECTURE NOTES IN ARTIFICIAL INTELLIGENCE AND LECTURE NOTES IN BIOINFORMATICS), ADVANCES IN INTELLIGENT SYSTEMS AND COMPUTING, COMMUNICATIONS IN COMPUTER AND INFORMATION SCIENCE, ACM INTERNATIONAL CONFERENCE PROCEEDING SERIES, JOURNAL OF PHYSICS: CONFERENCE SERIES, APPLIED SCIENCES (SWITZERLAND), IEEE ACCESS 2020 4TH INTERNATIONAL CONFERENCE ON ELECTRONICS, MATERIALS ENGINEERING AND NANO-TECHNOLOGY, IEMENTECH 2020* are some of the leading sources that are publishing the quality of research papers in the field of retail sector.

B. Authors and Country Distribution

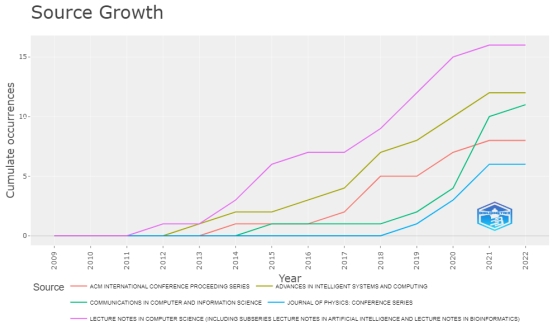
In this subsection, we give statistical details about the authors who are actively working to study the impact of cutting-



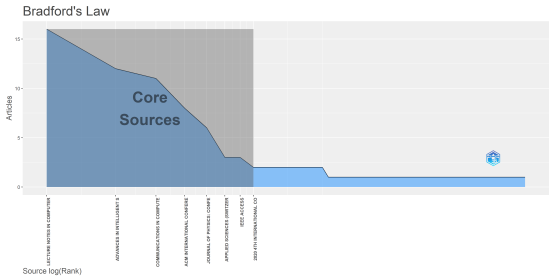
(a) Most cited sources



(b) Source distribution according to publication



(c) Source growth



(d) Bradford's Law

Fig. 2: Source Distribution

edge technologies on XSS attack detection. There are many ways through which we can find the most productive authors in the respective field. One method is the classification of authors by the number of citations. The Figure 3 represents the statics of the author. In Figure 3a the authors are represented through the frequency of article factorization, and in Figure 3b the authors most cited are represented. Therefore, from Figure 3a and Figure 3b it is clear that *CUI B, HOWE JM HUANG C, MEREANI FA, CHAUDHARY P, FANG Y, LI Y, SHAR LK, ZHOU Y, ABDULLAH J* are the authors who actively work in the field.

Apart from the number of citations, frequency and reverence are also the variables via which the most renowned authors in a particular subject may be determined. This analysis is presented in Figure 3c and **??**. From Figure 3c it is clear that as the year goes on, more and more research is interested in the respective research field. In 2020, only five researchers are working in the field, but in 2021, more than 10 researchers started their research in the respective domain. This also shows that this research topic is still developing and there is a scope of research in this domain. Finally, **??** represents the work area of the authors, and this figure is constructed on the principles of Sankey diagrams. From **??** it is clear that *Fleischmann D* and *Gopalkrishna P* work in the most diverse field. The research fields of the leading researchers are represented in **??**.

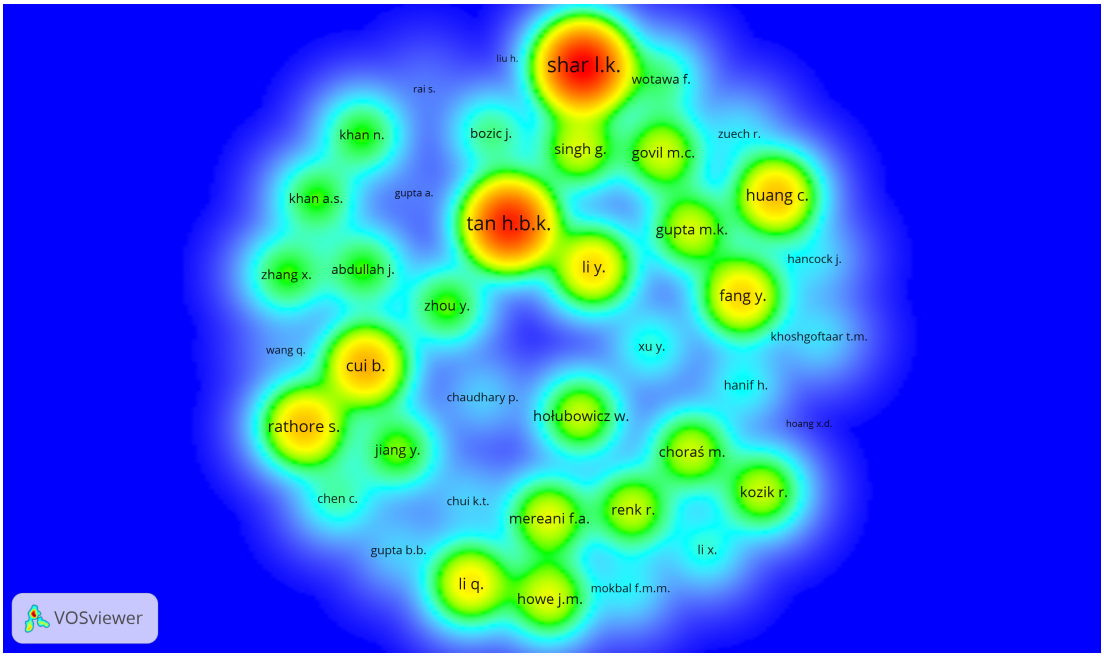
The distribution of researchers by nations is also a significant and beneficial component of the biblomatrix. This metric indicates the effectiveness of a country's researchers. Figure 4 represents the distribution of countries according to the total number of publications in paper and the corresponding authors.

TABLE III: Source distribution

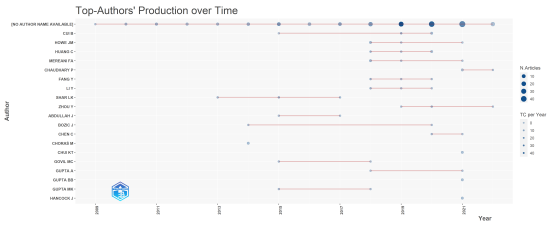
Element	h_index	g_index	m_index	TC	NP
SHAR LK	3	3	0.3	133	3
TAN HBK	2	2	0.2	115	2
NEUHAUS S	1	1	0.077	82	1
ZIMMERMANN T	1	1	0.077	82	1
BRIAND LC	1	1	0.125	66	1
CUI B	2	2	0.5	51	2
CHOI C	1	1	0.083	48	1
CHOI J	1	1	0.083	48	1
KIM H	1	1	0.083	48	1
KIM P	1	1	0.083	48	1
PARK JH	1	1	0.167	46	1
RATHORE S	1	1	0.167	46	1
SHARMA PK	1	1	0.167	46	1
HUANG C	3	4	0.6	45	4
DOS SANTOS EM	1	1	0.091	42	1
FEITOSA E	1	1	0.091	42	1
NUNAN AE	1	1	0.091	42	1
SOUTO E	1	1	0.091	42	1
YANG W	1	1	0.25	41	1
ZUO W	1	1	0.25	41	1

Figure 4 represents the top countries according to the paper publication frequency; according to the Figure 4 top ten countries with the most published articles, Figure 4 are:

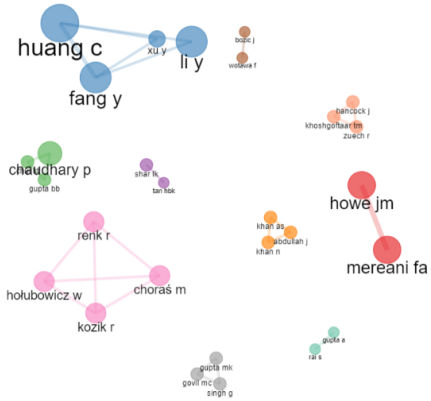
- *CHINA* (190)
- *ITALY* (94)
- *KOREA* (94)
- *LUXEMBOURG* (66)
- *SINGAPORE* (49)
- *USA* (46)
- *BRAZIL* (42)
- *JAPAN* (37)



(a) Authors according to citation



(b) Authors According to Citation



(c) Authors work over the years

Fig. 3: Authors Stastics

- *UNITED KINGDOM* (31)
- *INDIA* (21)

Therefore, from **??**, we can say that Indian researchers have been actively working in the field of the development of concepts for the retail sector for the past two years. The next important factor is the collaboration among the authors from different countries, which represents the productivity of a country. **??** represents the distribution of the corresponding authors and the nature of the paper (ie, single author (SCP) or multiauthor (MCP) paper). From the **??** it is clear that:

- The collaboration rates of authors from China, India, Iran, Italy, Korea, Poland, Norway, and the UK do not collaborating much.
- The 33% authors from the US are collaborating with the authors from other countries.
- More than 50% authors from Malaysia and Portugal are collaborating with other country authors.
- Finally, the authors of Finland and Ireland are working

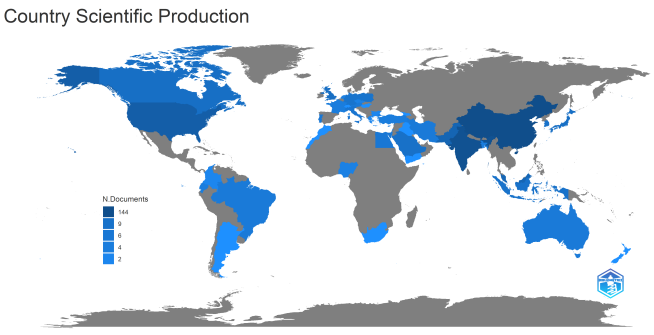


Fig. 4: Countries' Scientific Production

100% with other authors from countries.

C. Documents Distribution

In this subsection, we give details about the scientific distribution of the research papers. In the Scopus database, there are 184 articles related to our study. However, not all the published papers are important and provide valuable information about the subject area. Therefore, to obtain the information of the article, we find highly cited articles related to the development of XSS attack detection techniques. The details of this type of papers are presented in Figure 5 and Table IV. In Figure 5, the documents are represented according to the citation. Therefore, as the citation of the paper increases, it becomes darker. Similarly, Table IV arrange the papers according to total citations, average citation, and normalized citation.

IV. Conclusion

Using a bibliometric analysis, this study aims to assess the current state of the retail sector in light of the COVID-19 revisions, identify relevant problems and suggest future research challenges. As a result, our research has added to the body of knowledge in both the retail industry and the academic community.

In this review a large number of articles are included (96 in total, between 2009 and 2022). The progress of the retail sector under COVID-19 is thoroughly documented in a wide range of academic disciplines. E-Commerce and supply chain management, consumer behavior analysis, and AI-based decision making are just a few examples of research related to retail currently being conducted. Although this topic has only been around for around two years, scholars from a wide range of fields are taking an interest in it. Aside from geographical and intellectual diversity, this interest in retail is also visible in the contributions made by nations and institutions (the United States, China and India) of diverse origin. Furthermore, the number of papers and citations has grown exponentially in the last two years, leading us to believe that retail research is a growing trend. The rise in interest in retail is attributed to the introduction and implementation of cutting-edge technologies such as AI and ML in this sector. The most productive researchers actively working in this research field are: *FLEISCHMANN D*, *GOPALAKRISHNA P*, *LOPES M*, *ABBU HR*, and *ABDULLAH NS*. Based on co-occurrence analysis and the terms writers use to define their work, we have drawn together a pair of strategic diagrams that reveal both previously studied subjects and new research trends. The analysis shows that the most relevant themes studied in the current literature are retail stores, service industry, e-Commerce, supply chain management, sustainable development, behavioral analysis, and empirical analysis. Therefore, more frameworks and algorithms are needed to solve the issues related to these themes.

References

[1] M. Al-Ayyoub et al., "Accelerating 3d medical volume segmentation using gpus," *Multimedia Tools and Applications*, vol. 77, no. 4, pp. 4939–4958, 2018.

[2] A. Gaurav, K. Psannis, and D. Peraković, "Security of cloud-based medical internet of things (miots): A survey," *International Journal of Software Science and Computational Intelligence (IJSSCI)*, vol. 14, no. 1, pp. 1–16, 2022.

[3] A. M. Manasrah et al., "An optimized service broker routing policy based on differential evolution algorithm in fog/cloud environment," *Cluster Computing*, vol. 22, no. 1, pp. 1639–1653, 2019.

[4] B. B. Gupta, M. Misra, and R. C. Joshi, "An isp level solution to combat ddos attacks using combined statistical based approach. arxiv," 2012, preprint.

[5] S. R. Sahoo et al., "Fake profile detection in multimedia big data on online social networks," *International Journal of Information and Computer Security 12 (2-3)*, pp. 303–331, 2020.

[6] P. Chaudhary et al., "A framework for preserving the privacy of online users against xss worms on online social network," *International Journal of Information Technology and Web Engineering (IJITWE ...*, 2019.

[7] H. Fatemidokht et al., "Efficient and secure routing protocol based on artificial intelligence algorithms with uav-assisted for vehicular ad hoc networks in intelligent transportation systems," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 7, pp. 4757–4769, 2021.

[8] M. Chopra et al., "Analysis prognosis of sustainable development goals using big data-based approach during covid-19 pandemic," *Sustainable Technology and Entrepreneurship*, vol. 1, no. 2, p. 100012, 2022.

[9] G. N. Nguyen, L. Viet, N. H., M. Elhoseny, K. Shankar, B. B. Gupta, and A. A. Abd El-Latif, "Secure blockchain enabled cyber–physical systems in healthcare using deep belief network with resnet model," *Journal of Parallel and Distributed Computing*, vol. 153, pp. 150–160, 2021.

[10] F. Mereani and J. Howe, "Preventing cross-site scripting attacks by combining classifiers," 2018, pp. 135–143. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85059155733&doi=10.5220%2f0006894901350143&partnerID=40&md5=bd4246740d4d7702ff3449c8d490aaa6

[11] B. B. Gupta, S. Gupta, S. Gangwar, M. Kumar, and P. K. Meena, "Cross-site scripting (xss) abuse and defense: exploitation on several testing bed environments and its defense," *Journal of Information Privacy and Security*, vol. 11, no. 2, pp. 118–136, 2015.

[12] B. B. Gupta, P. Chaudhary, and S. Gupta, "Designing a xss defensive framework for web servers deployed in the existing smart city infrastructure," *Journal of Organizational and End User Computing (JOEUC)*, vol. 32, no. 4, pp. 85–111, 2020.

[13] S. Gupta et al., "Evaluation and monitoring of xss defensive solutions: a survey, open research issues and future directions," *Journal of ambient intelligence and humanized computing*, vol. 10, no. 11, pp. 4377–4405, 2019.

[14] P. Chaudhary et al., "Enhancing big data security through integrating xss scanner into fog nodes for smes gain," *Technological Forecasting and Social Change*, vol. 168, pp. 120 754–120 754, 2021.

[15] Pooja, *XSS Prevention Measures*. insights2techinfo.com. [Online]. Available: https://insights2techinfo.com/xss-prevention-measures/

[16] A. Mishra et al., "A comparative study of distributed denial of service attacks, intrusion tolerance and mitigation techniques," *In European Intelligence and Security Informatics Conference, . IEEE*, vol. 2011, pp. 286–289, 2011.

[17] A. Mishra et al., "Defense mechanisms against ddos attack based on entropy in sdn-cloud using pox controller," *Telecommunication systems*, vol. 77, no. 1, pp. 47–62, 2021.

[18] B. B. Gupta, A. Dahiya, C. Upneja, A. Garg, and R. Choudhary, "A comprehensive survey on ddos attacks and recent defense mechanisms," *Handbook of Research on Intrusion Detection Systems*, pp. 186–218, 2020.

[19] Z. Zhou et al., "A statistical approach to secure health care services from ddos attacks during covid-19 pandemic," *Neural Computing and Applications*, pp. 1–14, 2021.

[20] A. Gaurav et al., "Filtering of distributed denial of services (ddos) attacks in cloud computing environment," in *2021 IEEE International Conference on Communications Workshops (ICC Workshops)*. IEEE, 2021, pp. 1–6.

[21] P. Gulihar and B. B. Gupta, "Cooperative mechanisms for defending distributed denial of service (ddos) attacks," in *Handbook of Computer Networks and Cyber Security . , Cham*. Springer, 2020, pp. 421–443.

[22] B. B. Gupta and A. Dahiya, *Distributed Denial of Service (DDoS) Attacks: Classification, Attacks, Challenges and Countermeasures*. CRC press, 2021.

[23] A. Singh et al., "Distributed denial-of-service (ddos) attacks and defense mechanisms in various web-enabled computing platforms: Issues,

TABLE IV: Highely Cited Papers

Paper	DOI	Total Citations	TC per Year	Normalized TC
NEUHAUS S, 2010, PROC INT SYMP SOFTW RELIAB ENG[80]	10.1109/ISSRE.2010.53	82	6.308	2
SHAR LK, 2015, IEEE TRANS DEPENDABLE SECURE COMPUT [81]	10.1109/TDSC.2014.2373377	66	8.25	4.0135
SHAR LK, 2013, INF SOFTWARE TECHNOL [82]	10.1016/j.infsof.2013.04.002	49	4.9	2.7222
CHOI J, 2011, PROC - INT CONF NETW-BASED INF SYST, NBIS [83]	10.1109/NBiS.2011.104	48	4	1.5158
RATHORE S, 2017, J INF PROCESS SYST [84]	10.3745/JIPS.03.0079	46	7.667	4.4878
NUNAN AE, 2012, PROC IEEE SYMP COMPUT COMMUN [85]	10.1109/ISCC.2012.6249380	42	3.818	2.52
YANG W, 2019, IEEE ACCESS [86]	10.1109/ACCESS.2019.2895751	41	10.25	5.3838
FENG F, 2019, AD HOC NETW [87]	10.1016/j.adhoc.2018.09.014	40	10	5.2525
KOMIYA R, 2011, PROC INT CONF AWARE SCI TECHNOL, ICAST [88]	10.1109/ICAwST.2011.6163109	37	3.083	1.1684
RODRÍGUEZ GE, 2020, COMPUT NETWORKS [**?**]	10.1016/j.comnet.2019.106960	34	11.333	10.064
FANG Y, 2018, ACM INT CONF PROC SER [89]	10.1145/3194452.3194469	32	6.4	6.0952
GUO X, 2015, PROC - INT CONF CYBER-ENABLED DISTRIB COMPUT KNOWL DISCOV, CYBERC [90]	10.1109/CyberC.2015.50	31	3.875	1.8851
WANG R, 2014, PROC - IEEE INT CONF HIGH PERFORM COMPUT COMMUN, HPCC, IEEE INT CONF EMBED SOFTW SYST, ICESS INT SYMP CYBERSPACE SAF SECUR, CSS[56]	10.1109/HPCC.2014.137	23	2.556	1.6197
GUPTA MK, 2015, PROC INT JT CONF COMPUT SCI SOFTW ENG, JCSSE [91]	10.1109/JCSSE.2015.7219789	23	2.875	1.3986
MEREANI FA, 2018, ADV INTELL SYS COMPUT [92]	10.1007/978-3-319-74690-6_20	21	4.2	4
ARGYROS G, 2016, PROC - IEEE SYMP SECUR PRIVACY, SP [93]	10.1109/SP.2016.14	20	2.857	3.4146
ABAIMOV S, 2019, IEEE ACCESS [94]	10.1109/ACCESS.2019.2939870	18	4.5	2.3636
THOME J, 2017, PROC - IEEE/ACM INT CONF SOFTW ENG, ICSE	10.1109/ICSE.2017.26	18	3	1.7561
KRONJEE J, 2018, ACM INT CONF PROC SER [95]	10.1145/3230833.3230856	17	3.4	3.2381
PAN Y, 2019, J INTERNET SERV APPL [96]	10.1186/s13174-019-0115-x	17	4.25	2.2323
ZHANG X, 2020, IEEE ACCESS [97]	10.1109/ACCESS.2020.2965184	16	5.333	4.736
BLAND JA, 2020, COMPUT SECUR [98]	10.1016/j.cose.2020.101738	14	4.667	4.144
KOZIK R, 2014, ADV INTELL SYS COMPUT [99]	10.1007/978-3-319-07995-0_52	13	1.444	0.9155
KHAN N, 2015, INT CONF IT ASIA: TRANSFORM BIG DATA KNOWL, CITA - PROC [100]	10.1109/CITA.2015.7349842	13	1.625	0.7905
VISHNU BA, 2014, ACM INT CONF PROC SER [61]	10.1145/2660859.2660969	12	1.333	0.8451

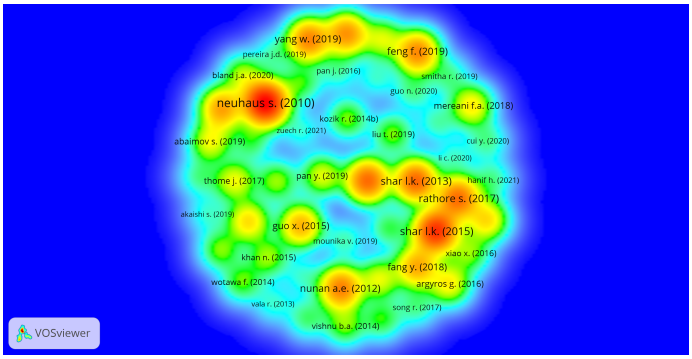


Fig. 5: Distribution of Documents

challenges, and future research directions," *International Journal on Semantic Web and Information Systems (IJSWIS)*, vol. 18, pp. 1–43, 2022.

[24] Z. Zhou et al., "A fine-grained access control and security approach for intelligent vehicular transport in 6g communication system," *IEEE transactions on intelligent transportation systems*, 2021.

[25] A. Gaurav et al., "A novel approach for ddos attacks detection in covid-19 scenario for small entrepreneurs," *Technological Forecasting and Social Change*, vol. 177, pp. 121 554–121 554, 2022.

[26] B. B. Gupta and A. K. Jain, "Phishing attack detection using a search engine and heuristics-based technique," *Journal of Information Technology Research (JITR)*, vol. 13, no. 2, pp. 94–109, 2020.

[27] A. Almomani et al., "Phishing website detection with semantic features based on machine learning classifiers: A comparative study," *International Journal on Semantic Web and Information Systems (IJSWIS)*, vol. 18, no. 1, pp. 1–24, 2022.

[28] S. Gupta et al., "A client-server javascript code rewriting-based framework to detect the xss worms from online social network," *Concurrency and Computation: Practice and Experience*, vol. 31, no. 21, p. 4646, 2019.

[29] B. Gupta, P. Chaudhary, and S. Gupta, "Designing a xss defensive framework for web servers deployed in the existing smart city infrastructure," *Journal of Organizational and End User Computing (JOEUC)*, vol. 32, no. 4, pp. 85–111, 2020.

[30] S. Gupta et al., "Evaluation and monitoring of xss defensive solutions: a survey, open research issues and future directions," *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, no. 11, pp. 4377–4405, 2019.

[31] P. Chaudhary et al., "Xsspro: Xss attack detection proxy to defend social networking platforms," *International Conference on Computational Data and Social Networks*, pp. 411–422, 2020.

[32] P. Chaudhary et al., "Securing heterogeneous embedded devices against xss attack in intelligent iot system," *Computers & Security*, vol. 118, pp. 102 710–102 710, 2022.

[33] P. Chaudhary et al., "Shielding smart home iot devices against adverse effects of xss using ai model," *2021 IEEE International Conference on Consumer Electronics (ICCE)*, pp. 1–5, 2021.

[34] P. B. B. Gupta, "Xsspro: Xss attack detection proxy to defend social networking platforms," *Computational Data and Social Networks*, pp. 411–422, 2021.

[35] B. P. Chaudhary, "Designing a xss defensive framework for web servers deployed in the existing smart cities infrastructure," *Journal of Organizational and End User Computing (JOEUC)*, 2019.

[36] Pooja, *What is Cross-Site Scripting (XSS) Worm?* insights2techinfo.com. [Online]. Available: https://insights2techinfo.com/what-is-cross-site-scripting-xss-worm/

[37] P. Chaudhary, *DOM-based Cross-Site Scripting Attack*. insights2techinfo.com. [Online]. Available: https://insights2techinfo.com/dom-based-cross-site-scripting-attack/

[38] G. Kaur, Y. Malik, H. Samuel, and F. Jaafar, "Detecting blind cross-site scripting attacks using machine learning," 2018, pp. 22–25. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85062781963&doi=10.1145%2f3297067.3297096&partnerID=40&md5=15b67c47ed45734c3c0fa2e90dc42be8

[39] A. Tewari et al., "A lightweight mutual authentication protocol based on elliptic curve cryptography for iot devices," *International Journal of Advanced Intelligence Paradigms*, vol. 9, no. 2-3, pp. 111–121, 2017.

[40] F. Mirsadeghi, M. K. Rafsanjani, and B. B. Gupta, "A trust infrastructure based authentication method for clustered vehicular ad hoc networks," *Peer-to-Peer Networking and Applications*, vol. 14, no. 4, pp. 2537–2553, 2021.

[41] T. Akhtar et al., "Malware propagation effects on scada system and smart power grid," in *2018 IEEE International Conference on Consumer Electronics (ICCE)*. IEEE, 2018, pp. 1–6.

[42] A. Tewari et al., "A lightweight mutual authentication approach for rfid tags in iot devices," *International Journal of Networking and Virtual Organisations*, vol. 18, no. 2, pp. 97–111, 2018.

[43] A. Gaurav et al., "A novel approach for fake news detection in vehicular ad-hoc network (vanet)," in *International conference on computational data and social networks*. Springer, 2020, pp. 386–397.

[44] Z. Wang et al., "Cloud-based federated boosting for mobile crowdsensing. arxiv," 2020, preprint.

[45] A. Tewari et al., "An internet-of-things-based security scheme for healthcare environment for robust location privacy," *International Journal of Computational Science and Engineering*, vol. 21, no. 2, pp. 298–303, 2020.

[46] A. Gaurav et al., "Ddos attack detection in vehicular ad-hoc network (vanet) for 5g networks," *Security and Privacy Preserving for IoT and 5G Networks*, pp. 263–278, 2022.

[47] A. Mishra, *Social And Web Analytics*. insights2techinfo.com. [Online]. Available: https://insights2techinfo.com/social-and-web-analytics/

[48] S. Sahoo et al., "Classification of various attacks and their defence mechanism in online social networks: a survey," *Enterprise Information Systems*, vol. 13, no. 6, pp. 832–864, 2019.

[49] Z. Zhang et al., "A crowdsourcing method for online social networks security assessment based on human-centric computing," *Human-centric Computing and Information Sciences*, vol. 10, no. 1, pp. 1–19, 2020.

[50] S. Sahoo et al., "Classification of spammer and nonspammer content in online social network using genetic algorithm-based feature selection," *Enterprise Information Systems*, vol. 14, no. 5, pp. 710–736, 2020.

[51] S. Sahoo et al., "Behavioral analysis to detect social spammer in online social networks (osns)," *International Conference on Computational Data and Social Networks*, pp. 321–332, 2020.

[52] S. R. Sahoo et al., "Detection of spammer account through rumor analysis in online social networks," *The 9th international conference on smart media and applications, n/a*, 2020.

[53] B. Gupta and S. Sahoo, *Online Social Networks Security: Principles, Algorithm, Applications, and Perspectives*. CRC Press, 2021.

[54] A. Mishra et al., "Entropy based defensive mechanism against ddos attack in sdn-cloud enabled online social networks," *2021 IEEE International Conference on Consumer Electronics (ICCE)*, pp. 1–6, 2021.

[55] B. Gupta, S. Sahoo, P. Chugh, V. Iota, and A. Shukla, "Defending multimedia content embedded in online social networks (osns) using digital watermarking," *Handbook of Research on Multimedia Cyber Security*, pp. 90–113, 2020.

[56] R. Wang, X. Jia, Q. Li, and S. Zhang, "Machine learning based cross-site scripting detection in online social network," 2014, pp. 823–826. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84949925441&doi=10.1109%2fHPCC.2014.137&partnerID=40&md5=6e2f12754898435d042bcbf71657863b

[57] U. S. Yadav et al., "Security and privacy of cloud-based online online social media: A survey," *Sustainable Management of Manufacturing Systems in Industry 4*, pp. 213–236, 2022.

[58] P. Gunti et al., "Data mining approaches for sentiment analysis in online social networks (osns)," *Data Mining Approaches for Big Data and Sentiment Analysis in Social Media ...*, 2022.

[59] A. Gaurav et al., "A novel approach for fake comments and reviews detection on the online social networks," *International Conference on Smart Systems and Advanced Computing (Syscom-2021)*, 2021.

[60] S. B. B. Gupta, *Online Social Networks Security: Principles, Algorithm, Applications, and Perspectives*. CRC Press, Taylor & Fancis 1, 122 pages, 2021.

[61] B. Vishnu and K. Jevitha, "Prediction of cross-site scripting attack using machine learning algorithms," vol. 10-11-October-2014, 2014. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84987834866&doi=10.1145%2f2660859.2660969&partnerID=40&md5=360c57bb58fb4aab01e8239134790483

[62] B. B. Gupta, V. Prajapati, N. Nedjah, P. Vijayakumar, A. A. A. El-Latif, and X. Chang, "Machine learning and smart card based two-factor authentication scheme for preserving anonymity in telecare medical information system (tmis)," *Neural Computing and Applications :*, pp. 1–26, 2021.

[63] A. Gaurav et al., "A comprehensive survey on machine learning approaches for malware detection in iot-based enterprise information system," *Enterprise Information Systems*, pp. 1–25, 2022.

[64] B. S. R. Sahoo, "Behavioral analysis to detect social spammer in online social networks (osns)," *Computational Data and Social Networks*, pp. 321–332, 2021.

[65] A. Gaurav et al., "Machine learning technique for fake news detection using text-based word vector representation," *International Conference on Computational Data and Social Networks*, pp. 340–348, 2021.

[66] M. Arowolo et al., "Machine learning-based iot system for covid-19 epidemics," *Computing*, pp. 1–17, 2022.

[67] C. Li, Y. Wang, C. Miao, and C. Huang, "Cross-site scripting guardian: A static xss detector based on data stream input-output association mining," *Applied Sciences (Switzerland)*, vol. 10, no. 14, 2020. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85088629208&doi=10.3390%2fapp10144740&partnerID=40&md5=3779bb9cfddcf4c0234a64670028d6c8

[68] I. Tariq, M. Sindhu, R. Abbasi, A. Khattak, O. Maqbool, and G. Siddiqui, "Resolving cross-site scripting attacks through genetic algorithm and reinforcement learning," *Expert Systems with Applications*, vol. 168, 2021. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85097341143&doi=10.1016%2fj.eswa.2020.114386&partnerID=40&md5=85d3cf6a2e03278157d71e889270ff5b

[69] K. Chui et al., "A genetic algorithm optimized rnn-lstm model for remaining useful life prediction of turbofan engine," *Electronics*, vol. 10, no. 3, pp. 285–285, 2021.

[70] M. Ajmal et al., "Hybrid ant genetic algorithm for efficient task scheduling in cloud data centers," *Computers & Electrical Engineering*, vol. 95, pp. 107 419–107 419, 2021.

[71] C. Stergiou et al., "Secure machine learning scenario from big data in cloud computing via internet of things network," *Handbook of Computer Networks and Cyber Security*, pp. 525–554, 2020.

[72] B. Gupta and Q. Sheng, *Machine learning for computer and cyber security: principle, algorithms, and practices*. CRC Press, 2019.

[73] K. Sharma et al., "Towards privacy risk analysis in android applications using machine learning approaches," *International Journal of E-Services and Mobile Applications (IJESMA) 11 (2 ...*, 2019.

[74] S. Sahoo et al., "Popularity-based detection of malicious content in facebook using machine learning approach," *First International Conference on Sustainable Technologies for Computational ...*, 2020.

[75] B. Gupta, V. Prajapati, N. Nedjah, P. Vijayakumar, A. El-Latif, and X. Chang, "Machine learning and smart card based two-factor authentication scheme for preserving anonymity in telecare medical information system (tmis)," *Neural Computing and Applications*, pp. 1–26, 2021.

[76] K. Yadav et al., "Differential privacy approach to solve gradient leakage attack in a federated machine learning environment," *International Conference on Computational Data and Social Networks*, pp. 378–385, 2020.

[77] K. Yadav et al., "Clustering based rewarding algorithm to detect adversaries in federated machine learning based iot environment," *2021 IEEE International Conference on Consumer Electronics (ICCE)*, pp. 1–6, 2021.

[78] B. Gupta and M. Sheng, "Machine learning for computer and cyber security," 2019.

[79] P. Nagarjun and S. Ahamad, "Ensemble methods to detect xss attacks," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 5, pp. 695–700, 2020. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85085748056&doi=10.14569%2fIJACSA.2020.0110585&partnerID=40&md5=f01ae53a54b7a3682d320ecb2fe33e6b

[80] S. Neuhaus and T. Zimmermann, "Security trend analysis with cve topic models," 2010, pp. 111–120. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-79952030607&doi=10.1109%2fISSRE.2010.53&partnerID=40&md5=2379ad77e94d908f32993e4fc73452c4

[81] L. Shar, L. Briand, and H. Tan, "Web application vulnerability prediction using hybrid program analysis and machine learning," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 6, pp. 688–707, 2015. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84959283014&doi=10.1109%2fTDSC.2014.2373377&partnerID=40&md5=e64a056f2cebaef93063019958a56170

[82] L. Shar and H. Tan, "Predicting sql injection and cross site scripting vulnerabilities through mining input sanitization patterns," *Information and Software Technology*, vol. 55, no. 10, pp. 1767–1780, 2013. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84880843062&doi=10.1016%2fj.infsof.2013.04.002&partnerID=40&md5=077d790d98cf2de91099555f65577ced

[83] J. Choi, C. Choi, H. Kim, and P. Kim, "Efficient malicious code detection using n-gram analysis and svm," 2011, pp. 618–621. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-80455144849&doi=10.1109%2fNBiS.2011.104&partnerID=40&md5=617c2f71a441b70affebe2e6f01eaec2

[84] S. Rathore, P. Sharma, and J. Park, "Xssclassifier: An efficient xss attack detection approach based on machine learning classifier on snss," *Journal of Information Processing Systems*, vol. 13, no. 4, pp. 1014–1028, 2017. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85029003429&doi=10.3745%2fJIPS.03.0079&partnerID=40&md5=fc70ce546eec119a751b76f157be9e2f

[85] A. Nunan, E. Souto, E. Dos Santos, and E. Feitosa, "Automatic classification of cross-site scripting in web pages using document-based and url-based features," 2012, pp. 000 702–000 707. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84866599219&doi=10.1109%2fISCC.2012.6249380&partnerID=40&md5=f4c24371019a9a68951efdbda1816dd9

[86] W. Yang, W. Zuo, and B. Cui, "Detecting malicious urls via a keyword-based convolutional gated-recurrent-unit neural network," *IEEE Access*, vol. 7, pp. 29 891–29 900, 2019. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85065224044&doi=10.1109%2fACCESS.2019.2895751&partnerID=40&md5=f6fb2f00313611a85d8ded570a585118

[87] F. Feng, X. Liu, B. Yong, R. Zhou, and Q. Zhou, "Anomaly detection in ad-hoc networks based on deep learning model: A plug and play device," *Ad Hoc Networks*, vol. 84, pp. 82–89, 2019. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85054705222&doi=10.1016%2fj.adhoc.2018.09.014&partnerID=40&md5=86befe017ea4afeeac427d87ed2a3b62

[88] R. Komiya, I. Paik, and M. Hisada, "Classification of malicious web code by machine learning," 2011, pp. 406–411. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84858761171&doi=10.1109%2fICAwST.2011.6163109&partnerID=40&md5=b0056b706e85a7ee98a1e6ecf07e6e17

[89] Y. Fang, Y. Li, L. Liu, and C. Huang, "Deepxss: Cross site scripting detection based on deep learning," 2018, pp. 47–51. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85048363065&doi=10.1145%2f3194452.3194469&partnerID=40&md5=ae8fd576c5386bc4a210e1ae30f3601c

[90] X. Guo, S. Jin, and Y. Zhang, "Xss vulnerability detection using optimized attack vector repertory," 2015, pp. 29–36. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84962597640&doi=10.1109%2fCyberC.2015.50&partnerID=40&md5=e04095451382b1726470b837aceec56e

[91] M. Gupta, M. Govil, and G. Singh, "Predicting cross-site scripting (xss) security vulnerabilities in web applications," 2015, pp. 162–167. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84945944571&doi=10.1109%2fJCSSE.2015.7219789&partnerID=40&md5=4915b7101ceb30ee9753d0cf644c29e0

[92] F. Mereani and J. Howe, "Detecting cross-site scripting attacks using machine learning," *Advances in Intelligent Systems and Computing*, vol. 723, pp. 200–210, 2018. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85041803514&doi=10.1007%2f978-3-319-74690-6_20&partnerID=40&md5=c888a0edabcbefef266049e828ae7c7c

[93] G. Argyros, I. Stais, A. Kiayias, and A. Keromytis, "Back in black: Towards formal, black box analysis of sanitizers and filters,"

2016, pp. 91–109. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84987608764&doi=10.1109%2fSP.2016.14&partnerID=40&md5=5eeb8737b1bff2ea2d099ae9c7697024

[94] S. Abaimov and G. Bianchi, "Coddle: Code-injection detection with deep learning," *IEEE Access*, vol. 7, pp. 128 617–128 627, 2019. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85078242989&doi=10.1109%2fACCESS.2019.2939870&partnerID=40&md5=c510a0e63d4913e5061e8b2d25d7c591

[95] J. Kronjee, A. Hommersom, and H. Vranken, "Discovering software vulnerabilities using data-flow analysis and machine learning," 2018. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85055270893&doi=10.1145%2f3230833.3230856&partnerID=40&md5=a08f210d2bf926c66a45e2a6825fd9ff

[96] Y. Pan, F. Sun, Z. Teng, J. White, D. Schmidt, J. Staples, and L. Krause, "Detecting web attacks with end-to-end deep learning," *Journal of Internet Services and Applications*, vol. 10, no. 1, 2019. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85071595946&doi=10.1186%2fs13174-019-0115-x&partnerID=40&md5=167fffb1be38e30c5c35e73a7e54a545

[97] G. Wang, Z. Wu, X. Zhang, and H. Dong, "A double correction of d-s evidence theory for information authenticity screening," 2019, pp. 1470–1474. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85071130159&doi=10.1109%2fITAIC.2019.8785511&partnerID=40&md5=2852c86dd2f9e3f798bd6d59b6afe103

[98] J. Bland, M. Petty, T. Whitaker, K. Maxwell, and W. Cantrell, "Machine learning cyberattack and defense strategies," *Computers and Security*, vol. 92, 2020. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85079088937&doi=10.1016%2fj.cose.2020.101738&partnerID=40&md5=e0fccd7575b51a5227c6a551149b30df

[99] R. Kozik, M. Choraś, R. Renk, and W. Hołubowicz, "Modelling http requests with regular expressions for detection of cyber attacks targeted at web applications," *Advances in Intelligent Systems and Computing*, vol. 299, pp. 527–535, 2014. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84927728566&doi=10.1007%2f978-3-319-07995-0_52&partnerID=40&md5=6ec340e17c436140800452bf83441f8e

[100] N. Khan, J. Abdullah, and A. Khan, "Towards vulnerability prevention model for web browser using interceptor approach," 2015. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84962850111&doi=10.1109%2fCITA.2015.7349842&partnerID=40&md5=c53cd328673fa4c8d74345b092e9f7cb